

**Noiseless coding theorem proved by induction
for finite stationary memoryless information sources**

Jozsef Szabo

Tampere University of Technology

PL 553, 33101 Tampere, Finland

jozsef.szabo@tut.fi

5 July 2014

Abstract

Noiseless coding theorem for finite stationary memoryless information sources is proved by using induction on the number of source symbols and the inequality of geometric and harmonic means.

1. Introduction, terminology, notation

The noiseless coding theorem is well known since Shannon's work ([S1]). The noiseless coding theorem for finite memoryless stationary information sources is a special case of the general noiseless coding theorem. It assumes that the information source is restricted such that it outputs only symbols from a finite alphabet and each outputted symbol has the same probability distribution (the source is stationary) with no correlation between outputted symbols at different time (the source is memoryless). The theorem gives a lower bound of the average codeword length of any uniquely decipherable code used for encoding the data coming from an information source with these restricted properties.

Unlike the proofs using analysis ([MK6] and [R5]) here is given a proof using induction based on the number source symbols. We represent an information source (or shortly source) of this kind (S, P) (or shortly S) where $S = \{s_1, \dots, s_n\}$ is the source alphabet and $P = \{\{p_1, \dots, p_n\}\}$, $\sum_{i=1}^n p_i = 1$, $p_i \in \mathbb{R}_+^*$, where p_i is the probability of outputting a source symbol s_i , $i = 1 \dots n$.

We represent an r -ary code corresponding to source S by (C, f) (or shortly C) where $C = \{c_1, \dots, c_m\}$, $c_j \in A^*$ ($A^* = A^0 \cup A^1 \cup \dots$ is the Kleene closure), $j = 1 \dots m$, where $A = \{0, \dots, r-1\}$ an r -ary alphabet, $r \in \mathbb{N}^*$ and $f: S \rightarrow \wp(C) \setminus \{\emptyset\}$ is a function which for each source symbols defines the set of codewords from which one can be used at any time to encode that source symbol. It is usually assumed that $\text{card } f(s_i) = 1$, $\forall i = 1 \dots n$, but that is not enforced by any means.

For the code C to be non-singular (non-ambiguous) we need to assume $f(s_i) \cap f(s_j) = \emptyset$, $\forall i \neq j$ where $i, j = 1 \dots n$. This implies that we have $\text{card } S \leq \text{card } C$ ($n \leq m$).

A non-singular code C of S , where $\text{card } S = \text{card } C$ ($\text{card } f(s_i) = 1$, $\forall i = 1 \dots n$) is called uniquely decipherable if $\forall w \in C^*$ (C^* is the Kleene closure) is a unique concatenation of codewords from C and is called instantaneous if non of the codewords in the code are prefixes of each other. These concepts can be extended to the case when $\text{card } S \leq \text{card } C$ ($\text{card } f(s_i) \geq 1$, $\forall i = 1 \dots n$). We could then define C to be uniquely decipherable if $\forall w \in C^*$ (C^* is the Kleene closure) all the possible representation of w as concatenation of codewords correspond to (decodes to) a unique sequence of source word $s \in S^*$; and we could define C to be instantaneous if non of the codewords in the code are prefixes of each other (same definition as before).

Let us use the notation $H_r(S)$ for the r -ary entropy ($r \in \mathbb{N}^*$) of the finite stationary memoryless source (S, P) .
 $H_r(S) = - \sum_{i=1}^n p_i \cdot \log_r(p_i)$, $n = \text{card } S$.

Let us also use the notation $ACL_r(S, C)$ for the average codeword length of any r -ary code C of S . $ACL_r(S, C) = \sum_{i=1}^n p_i \cdot l_i$ when $\forall i = 1 \dots n : \text{card } f(s_i) = 1$ where $L = \{l_1, \dots, l_n\}$ where $l_i = \text{length}(c_i)$, $c_i \in f(s_i)$, $i = 1 \dots n$.

More generally if $\text{card } f(s_i) \geq 1$ we can say that $ACL_r(S, C) = \sum_{i=1}^n p_i \cdot (\sum_{u=1}^{\text{card } f(s_i)} q_{i,u} \cdot l_{i,u})$, when $q_{i,u}$ are well defined probabilities of encoding s_i by $c_{i,u} \in f(s_i)$, $\sum_{u=1}^{\text{card } f(s_i)} q_{i,u} = 1$, $q_{i,u} > 0$, $\forall u = 1 \dots \text{card } f(s_i)$ and $L = \{l_{1,1}, \dots, l_{1,\text{card } f(s_1)}, \dots, l_{n,1}, \dots, l_{n,\text{card } f(s_n)}\}$ where $l_{i,u} = \text{length}(c_{i,u})$, $c_{i,u} \in A^*$, $i = 1 \dots n$; $j = 1 \dots m$.

If any of the $q_{i,u}$ probabilities doesn't exist then average codeword length cannot be defined as such. In that case,

we can take the sequence $ACL_{r,t}(S, C) = \frac{\sum_{i=1}^n (\sum_{z=1}^t \sum_{u=1}^{\text{card } f(s_i)} k_{i,u,z} \cdot l_{i,u})}{t}$ of average codeword lengths after

encoding t source symbols, $f_{i,t} = \sum_{z=1}^t \sum_{u=1}^{\text{card } f(s_i)} k_{i,u,z}$ is the frequency of the source outputting s_i when outputting t symbols and $k_{i,u,z} = 1$ if the z^{th} outputted symbol is s_i and is encoded to $c_{i,u}$ and otherwise $k_{i,u,z} = 0$. This sequence is kind of bounded below as follows:

$$\begin{aligned} ACL_{r,t}(S, C) &\geq \frac{\sum_{i=1}^n (\sum_{z=1}^t \sum_{u=1}^{\text{card } f(s_i)} k_{i,u,z} \cdot \min_{u=1 \dots \text{card } f(s_i)} l_{i,u})}{t} \\ &= \frac{\sum_{i=1}^n \min_{u=1 \dots \text{card } f(s_i)} l_{i,u} \cdot (\sum_{z=1}^t \sum_{u=1}^{\text{card } f(s_i)} k_{i,u,z})}{t} \\ &= \frac{\sum_{i=1}^n l_i \cdot (\sum_{z=1}^t \sum_{u=1}^{\text{card } f(s_i)} k_{i,u,z})}{t} = \\ &= \frac{\sum_{i=1}^n f_{i,t} \cdot l_i}{t} = ACL_{r,t}(S, C'), \end{aligned}$$

where (C', g) is another encoding for the source S where $g(s_i) = c_{i,u} \in f(s_i)$ for which $\text{length}(c_i) = l_i = \min_{u=1 \dots \text{card } f(s_i)} l_{i,u}$.

It is clear that $\lim_{t \rightarrow \infty} ACL_{r,t}(S, C') = ACL_r(S, C')$.

So we have $ACL_{r,t}(S, C) \geq ACL_r(S, C')$ if t is big enough and so we could say formally $ACL_r(S, C) \geq ACL_r(S, C')$, even if it $ACL_{r,t}(S, C)$ doesn't converge to an exact value when $t \rightarrow \infty$. Let us rely in our proof on the results obtained by Kraft ([K2] and [R5]) and McMillan ([M4] and [R5]).

The proof that any extension of the source S to the source S^p etc. will not give better average codeword length either than the entropy of S can be revisited elsewhere ([R5]). This is due to fact the property holds for S (see our proof from 2.) and from the fact that the source is assumed to be memoryless ([R5]).

2. Statement of the discrete noiseless coding theorem

Theorem: If (S, P) is a finite stationary memoryless information source then $H_r(S) \leq ACL_r(S, C), \forall C$ uniquely decipherable code of S .

Proof.

It is obvious that it is enough to consider only the case when $\text{card } C = \text{card } S$ ($m = n$) without any loss of generality because for every code (C, f) with $\text{card } C = m > n$ can always be constructed a code (C', g) , $\text{card } C' = n$ for which holds $ACL_r(S, C') \leq ACL_r(S, C)$. This as for $\forall s_i, i = 1 \dots n$ we can define for $\forall i = 1 \dots n$: $g(s_i) = \{c_{i_k}\}$, where $f(s_i) = \{c_{i_1}, \dots, c_{i_v}\}$ and $l_{i_k} = \min_{u=1 \dots v} l_{i_u}$, $l_{i_u} = \text{length}(c_{i_u})$, $u = 1 \dots v$ (see also for details above in 1.).

If $r = 1$ is obvious that $H_r(S) = -1 \cdot \log_r(1) = 0$ since the only possible uniquely decipherable codes are the form $C = \{c_1\}$, $c_1 \in A^* (A = \{0\})$. Equality would hold only if $l_1 = 0$ which means $c_1 = \lambda \epsilon A^*$ which is practically useless.

Next on we assume $r \geq 2$.

Due to Kraft's and McMillan's theorems it holds for every r -ary uniquely decipherable code C of source S it is possible to construct an instantaneous code C' of S starting from the same codeword lengths ($\text{card } C' = \text{card } C$ and $\text{length}(c'_i) = \text{length}(c_i)$, $i = 1 \dots n$). This implies $ACL_r(S, C') = ACL_r(S, C)$ and therefore without loss of generality we can delimit ourselves to consider only instantaneous codes.

Due to Kraft's theorem for every r -ary instantaneous code it corresponds and r -ary tree and vice versa.

We will use induction over $\text{card } S$. To be able to apply the induction step from a code C of S where $\text{card } C \leq n$ to a code C' of S' with $\text{card } C' = n + 1$ we will need to do a reduction of a code of $n + 1$ elements to a code of n elements. This becomes possible if we could consider only such instantaneous codes for which the corresponding r -ary tree doesn't have any node(except the root) as standalone sibling node(standalone child node). It is known that for every r -ary tree which does have such nodes, by removing those we get an r -ary tree with smaller average codeword length ([H3], [R5]).

Finally, let us extend the set of special instantaneous codes for which we want to do induction with 1 more element, the code $C_\lambda = \{\lambda\}$ ($\lambda \in A^0$). This extension is required for the first step of the induction. That doesn't restrict the generality anyhow as we will prove the property for a bigger set than the special instantaneous codes.

If $\text{card } S = 1$ then $P = \{p_1 = 1\}$ and $C = \{\lambda\}$. So we have $H_r(S) = -p_1 \cdot \log_r(p_1) = -1 \cdot \log_r(1) = 0$, $ACL_r(S) = p_1 \cdot l_1 = 1 \cdot 0 = 0$. Here even equality holds.

So we can do strong induction as any restricted instantaneous code can be reduced to the code $C_\lambda = \{\lambda\}$ ultimately.

Let assume now that the inequality is true for any restricted and extended instantaneous code C (as above) of the source (S, P) where $\text{card } C \leq n$, $n \geq 1$ and let us prove it for a code C' of the source (S', P') where $\text{card } C' = n + 1$. Let us use the notations: $P' = \{p_1, p_2, \dots, p_{n+1}\}$ and $C' = \{x_1, x_2, \dots, x_{n+1}\}$ relative to S' .

Due to the special properties of the instantaneous codes considered there exists $x_{i_1}, x_{i_2}, \dots, x_{i_s}$, $2 \leq s \leq r$, where $\text{length } x_{i_j} = \text{length } x_{i_k} \forall j, k = 1 \dots s$ and the x_{i_k} -s, $k = 1 \dots s$ differ only in their last symbol (to them corresponds sibling leafs in the corresponding r -ary tree). Let us reduce (C', P') to (C_{red}, P_{red}) where $C_{red} = C' \cup \{x_{red}\} \setminus \{x_{i_1}, x_{i_2}, \dots, x_{i_s}\}$ and the x_{red} codeword is created by dropping the last symbol from any of the codewords x_{i_k} from C' , $k = 1 \dots s$.

P_{red} is formed by adding $p_{red} = p_{i_1} + \dots + p_{i_s}$ for x_{red} and keeping the probabilities unchanged from P' for the retained codewords from C' .

We have:

$$H_r(S') = H_r(S_{red}) + p_{red} \cdot \log_r(p_{red}) - p_{i_1} \cdot \log_r(p_{i_1}) - p_{i_2} \cdot \log_r(p_{i_2}) - \dots - p_{i_s} \cdot \log_r(p_{i_s})$$

$$ACL_r(S', C') = ACL_r(S_{red}, C_{red}) - p_{red} \cdot l_{red} + p_{i_1} \cdot l_{i_1} + p_{i_2} \cdot l_{i_2} + \dots + p_{i_s} \cdot l_{i_s} =$$

$$ACL_r(S_{red}, C_{red}) - p_{red} \cdot l_{red} + p_{i_1} \cdot (l_{red} + 1) + p_{i_2} \cdot (l_{red} + 1) + \dots + p_{i_s} \cdot (l_{red} + 1) =$$

$$ACL_r(S_{red}, C_{red}) + p_{red} \cdot l_{red} \text{ and by subtracting we get:}$$

$$H_r(S') - ACL_r(S', C') =$$

$$H_r(S_{red}) - ACL_r(S_{red}, C_{red}) + p_{red} \cdot \log_r(p_{red}) - p_{i_1} \cdot \log_r(p_{i_1}) - p_{i_2} \cdot \log_r(p_{i_2}) - \dots - p_{i_s} \cdot \log_r(p_{i_s}) - p_{red}$$

As $\text{card } C_{red} \leq n$ then the induction hypothesis is true for it: $H_r(S_{red}) - ACL_r(S_{red}, C_{red}) \leq 0$.

We only have to prove:

$$p_{red} \cdot \log_r(p_{red}) - p_{i_1} \cdot \log_r(p_{i_1}) - p_{i_2} \cdot \log_r(p_{i_2}) - \dots - p_{i_s} \cdot \log_r(p_{i_s}) - p_{red} \leq 0$$

to end the proof.

By rearranging we get equivalently:

$$\begin{aligned}
\log_r\left(\frac{p_{red}}{r}\right)^{p_{red}} &\leq \log(p_{i_1}^{p_{i_1}} \cdot p_{i_2}^{p_{i_2}} \cdots p_{i_s}^{p_{i_s}}) \\
&\Leftrightarrow \left(\frac{p_{red}}{r}\right)^{p_{i_1}+p_{i_2}+\dots+p_{i_s}} \leq p_{i_1}^{p_{i_1}} \cdot p_{i_2}^{p_{i_2}} \cdots p_{i_s}^{p_{i_s}} \\
&\Leftrightarrow \left(\frac{r \cdot p_{i_1}}{p_{red}}\right)^{p_{i_1}} \cdot \left(\frac{r \cdot p_{i_2}}{p_{red}}\right)^{p_{i_2}} \cdots \left(\frac{r \cdot p_{i_s}}{p_{red}}\right)^{p_{i_s}} \geq 1
\end{aligned}$$

Here we can assume first that $p_{i_1}, p_{i_2}, \dots, p_{i_s} \in \mathbb{Q}$. The general statement follows by continuity of the expression involved and the density of \mathbb{Q} in \mathbb{R} .

Thus $p_{i_k} = \frac{f_{i_k}}{F}$, where $F = f_{i_1} + \dots + f_{i_s}$ and f_{i_k} are positive integers, $k = 1 \dots s$.

We need to prove that:

$$\left(\frac{r \cdot f_{i_1}}{f_{red}}\right)^{f_{i_1}} \cdot \left(\frac{r \cdot f_{i_2}}{f_{red}}\right)^{f_{i_2}} \cdots \left(\frac{r \cdot f_{i_s}}{f_{red}}\right)^{f_{i_s}} \geq 1, \text{ where } f_{red} = p_{red} \cdot F.$$

Applying the inequality between geometric means and harmonic means to the following sequence which has F number of terms:

$$\begin{aligned}
&\frac{r \cdot f_{i_1}}{f_{red}}, \dots, \frac{r \cdot f_{i_1}}{f_{red}}, \frac{r \cdot f_{i_2}}{f_{red}}, \dots, \frac{r \cdot f_{i_2}}{f_{red}}, \dots, \frac{r \cdot f_{i_s}}{f_{red}}, \dots, \frac{r \cdot f_{i_s}}{f_{red}}, \text{ we get} \\
&\left(\frac{r \cdot f_{i_1}}{f_{red}}\right)^{f_{i_1}} \cdot \left(\frac{r \cdot f_{i_2}}{f_{red}}\right)^{f_{i_2}} \cdots \left(\frac{r \cdot f_{i_s}}{f_{red}}\right)^{f_{i_s}} = \\
&\left(\frac{r \cdot f_{i_1}}{f_{red}}\right) \cdots \left(\frac{r \cdot f_{i_1}}{f_{red}}\right) \left(\frac{r \cdot f_{i_2}}{f_{red}}\right) \cdots \left(\frac{r \cdot f_{i_2}}{f_{red}}\right) \cdots \left(\frac{r \cdot f_{i_s}}{f_{red}}\right) \cdots \left(\frac{r \cdot f_{i_s}}{f_{red}}\right) \geq \\
&\left(\frac{f_{i_1} + f_{i_2} + \dots + f_{i_s}}{\frac{1}{\frac{r \cdot f_{i_1}}{f_{red}}} + \dots + \frac{1}{\frac{r \cdot f_{i_1}}{f_{red}}} + \frac{1}{\frac{r \cdot f_{i_2}}{f_{red}}} + \dots + \frac{1}{\frac{r \cdot f_{i_2}}{f_{red}}} + \dots + \frac{1}{\frac{r \cdot f_{i_s}}{f_{red}}} + \dots + \frac{1}{\frac{r \cdot f_{i_s}}{f_{red}}}}\right)^{f_{i_1}+f_{i_2}+\dots+f_{i_s}} \\
&= \left(\frac{f_{red}}{\frac{f_{red}}{r \cdot f_{i_1}} \cdot f_{i_1} + \frac{f_{red}}{r \cdot f_{i_2}} \cdot f_{i_2} + \dots + \frac{f_{red}}{r \cdot f_{i_s}} \cdot f_{i_s}}}\right)^{f_{red}} \\
&= \left(\frac{r}{s}\right)^{f_{red}} \geq 1, \text{ just what we wanted to prove.}
\end{aligned}$$

Equality holds only if $p_{i_1} = \dots = p_{i_s}$ and $s = r$.

It easy to see that via induction that equality holds only if $p_{i_k} = \frac{1}{r^{i_k}}$, $\forall k = 1, n$ where $n = \text{card } S$ and also is of the form $n = z \cdot (r - 1) + 1$, $\forall n \geq 1$ where z is the number of internal nodes in the corresponding r -ary tree. If $\text{card } S = 1$, form $H(S) = ACL_r(S, C)$ we don't get new information as it holds anyway. Since $P = \{p_1 = 1\}$ we have $p_1 = \frac{1}{r^0}$ and $n = 1 = 0 \cdot (r - 1) + 1$.

Let us use strong induction as above and retain the notations from there.

For $\text{card } S' = n + 1$ from $H(S') = ACL_r(S', C')$ and doing same kind of reduction as for the proof above, we get:

$$H_r(S') - ACL_r(S', C') =$$

$$H_r(S_{red}) - ACL_r(S_{red}, C_{red}) + p_{red} \cdot \log_r(p_{red}) - p_{i_1} \cdot \log_r(p_{i_1}) - p_{i_2} \cdot \log_r(p_{i_2}) - \dots - p_{i_s} \cdot \log_r(p_{i_s}) - p_{red} \leq 0$$

since we proved already that

$$H_r(S_{red}) - ACL_r(S_{red}, C_{red}) \leq 0 \text{ and also that}$$

$$p_{red} \cdot \log_r(p_{red}) - p_{i_1} \cdot \log_r(p_{i_1}) - p_{i_2} \cdot \log_r(p_{i_2}) - \dots - p_{i_s} \cdot \log_r(p_{i_s}) - p_{red} \leq 0$$

it follows that both inequalities has to be equalities.

From $p_{red} \cdot \log_r(p_{red}) - p_{i_1} \cdot \log_r(p_{i_1}) - p_{i_2} \cdot \log_r(p_{i_2}) - \dots - p_{i_s} \cdot \log_r(p_{i_s}) - p_{red} = 0$ it follows that $s = r$ and $p_{i_j} = p_{i_k}, \forall j, k \leq s$, where $p_{red} = p_{i_1} + \dots + p_{i_s}$ as we saw in the proof of the theorem.

From $H_r(S_{red}) - ACL_r(S_{red}, C_{red}) = 0$ and because $\text{card } S_{red} \leq n$ the induction assumption is true, so

$$p_{red} = \frac{1}{r^{l_{red}}} \text{ since } p_v = \frac{1}{r^{l_v}}, \forall v = 1 \dots \text{card } S_{red} \text{ and also holds by induction assumption that}$$

$$\text{card } S_{red} = z \cdot (r - 1) + 1$$

$$\Rightarrow p_{red} = r \cdot p_{i_j} \Rightarrow p_{i_j} = \frac{p_{red}}{r} = \frac{1}{r^{l_{red}+1}} = \frac{1}{r^{l_{i_j}+1}}, \forall j = 1 \dots r$$

as well as for the rest of the values $p_v = \frac{1}{r^{l_v}}, \forall v = 1 \dots \text{card } S_{red}, v \neq \text{red}$ which are inherited by S' unchanged from $S \Rightarrow$ it is true for all probabilities of P' ; additionally

$\text{card } S' = \text{card } S_{red} + r - 1 = z \cdot (r - 1) + 1 + r - 1 = (z + 1) \cdot (r - 1) + 1$ which end the proof.

Let us observe that we got

$$\left(\frac{r \cdot p_1}{p_1 + \dots + p_s} \right)^{p_1} \cdot \left(\frac{r \cdot p_2}{p_1 + \dots + p_s} \right)^{p_2} \dots \left(\frac{r \cdot p_s}{p_1 + \dots + p_s} \right)^{p_s} \geq 1, \forall s = 1 \dots r \text{ and } \forall p_k \in \mathbb{R}_+^*, k = 1 \dots s$$

which is an interesting inequality as if we replace the powers $p_1 \dots p_s$ by 1 and if $s = r$ then the reverse inequality would hold,

because by rearranging $\left(\frac{r \cdot p_1}{p_1 + \dots + p_r} \right) \cdot \left(\frac{r \cdot p_2}{p_1 + \dots + p_r} \right) \dots \left(\frac{r \cdot p_r}{p_1 + \dots + p_r} \right) \leq 1$ we get the known inequality between arithmetic and geometric means.

Additionally we found that:

$$\left(\frac{p_1 + p_2 + \dots + p_s}{r} \right)^{p_1 + p_2 + \dots + p_s} \leq p_1^{p_1} \cdot p_2^{p_2} \dots p_s^{p_s}, \forall s = 1 \dots r \text{ and } \forall p_k \in \mathbb{R}_+^*, k = 1 \dots s \text{ and}$$

$$p_1^{p_1} \cdot p_2^{p_2} \dots p_s^{p_s} \geq \frac{1}{s}, \forall s \geq 1 \text{ integer and } \forall p_k \in \mathbb{R}_+^*, k = 1 \dots s \text{ where } p_1 + \dots + p_s = 1.$$

References

-
- [S1] Claude E. Shannon: A Mathematical Theory of Communication, Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, 1948.
- [K2] L.G. Kraft, A Device for Quantizing, Grouping, and Coding Amplitude Modulated Pulses, Q.S. Thesis, MIT, 1949.
- [H3] Huffman, D. (1952). "A Method for the Construction of Minimum-Redundancy Codes". Proceedings of the IRE 40 (9): 1098–1101. doi:10.1109/JRPROC.1952.273898
- [M4] B. McMillan, Two inequalities implied by unique decipherability, IRE Trans. Information Theory IT-2 (1956) 115-116
- [R5] Steven Roman, Coding and Information Theory, Springer 1992.
- [MK6] David MacKay, Information Theory, Inference and Learning Algorithms, Cambridge University Press 2003.